

Guide for Network Administrator's

First published for Skype for Windows version 3.0 (Dec 2006)

www.skype.biz

What is this Guide?

This guide provides information to help you understand how to manage Skype in the context of an enterprise environment.

Who should read this guide?

This *Network Administrator's Guide* is for IT personnel (system and network administrators) who are responsible for managing the deployment of software applications, specifically on the Microsoft Windows Platform.

This *Network Administrator's Guide* assumes you are familiar with enterprise deployment issues, editing the Windows registry, Windows Group Policy Administration, basic XML syntax, as well as other things related to networking and operating system environments.

Important legal information

Copyright

This document is the property of Skype Limited and its affiliated companies (Skype), and is protected by copyright and other intellectual property rights laws.

Skype makes no representation or warranty as to the accuracy, completeness, condition, suitability, or performance of this document or related documents or their content, and shall have no liability whatsoever to any party resulting from the use of any of such documents.

By using this document and any related documents, the recipient acknowledges Skype's intellectual property rights thereto and agrees to the terms above, and shall be liable to Skype for any breach thereof.

Trademarks

Skype is a trademark of Skype Limited. Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. Apple and Macintosh are registered trademarks of Apple Inc., registered in the United States and other countries.

All other names or brands may be trademarks or registered trademarks belonging to their respective owners.

Disclaimer

This document describes products offered by Skype Limited, its subsidiaries or affiliates as of the time of this writing. Skype products may be modified or terminated at any time according to the current End User License Agreement and Terms of Service, and any other applicable terms and conditions available at http://www.skype.com/legal. The internal design of Skype software and networking techniques are subject to change without prior notice.

Skype is not responsible for the content of any third-party websites or documents that may be referenced in this document. Any such references are provided purely for the convenience of Skype's customers, who are advised that Skype has not verified that such references are accurate or fit for any particular purpose.

What is in this Guide?

What is this Guide?	2
Who should read this guide?	2
Important legal information.	2
Copyright	2
Trademarks	
Disclaimer	2
What is in this Guide?	
Deploying Skype in the Enterprise	
General Guidelines	
Skype Client Notifications for New Versions and Updates	4
Enterprise-wide Installation and Setting Policies	
Policies	
Setting Up Group Policies	
Configurable Policies	
Registry Keys	

Deploying Skype in the Enterprise

Our goal is to enable users to enjoy Skype from as wide a variety of networks as possible, without requiring people to understand or configure complex options such as relay hosts or preferred network ports. In this sense, Skype is generally 'hands-off'.

The authentic and most up-to-date version of Skype is always available directly from Skype's own download server at http://www.skype.com/download. From here there is a business version available which includes the Windows Installer (MSI).

Once installed, the Skype client periodically checks to see if there is a software update available, although system- or network administrators may disable this feature. And end users can adjust their Skype client preferences to control how updates and patches are handled in general.

General Guidelines

Skype wants end users and enterprises alike to have a safe and enjoyable experience using Skype to enable communications. Toward this end, we would like to underscore the importance of keeping your company's computers and users safe and secure while doing so. Here are some of the main issues to be aware of:

- Before you deploy Skype in an organization, be sure it is an authentic copy. Check the
 digital signature of the installer and be sure to read and accept the terms and conditions
 in Skype's End User License Agreement and Terms of Service before deploying Skype
 software.
- Keep your organization's computers up-to-date with relevant patches. Most of the computer security problems on the Internet today can be traced back to improperly patched computers.
- Obvious as it may sound, use anti-virus protection, even on non-Microsoft computers

such as the Apple Macintosh, and keep the virus definitions constantly updated.

- When you use Skype, know who you're authorizing and don't hesitate to block users who are making unwanted contact. Keep user profiles up-to-date, but also know that everything in a user's profile (except e-mail addresses which are masked for privacy) are viewable to others whose search criteria matches the information in the profile. The Privacy Policy at http://www.skype.com/legal/privacy sets out how Skype may use end user's personal data, traffic data and the content contained in communication(s). You should ensure that end users have read and agree to this policy before using Skype.
- Always authenticate other parties before beginning to discuss any confidential business
 or sensitive personal information. Remember that although Skype takes care to protect
 communications from unwanted disclosure, there is the remote possibility that your
 computer, or those belonging to persons with whom you are communicating have been
 "hacked" or compromised in some way.
- Instruct your users to choose good passwords for Skype and change them regularly.
 Remember, users should never check "remember my password" when using Skype on a shared computer.

Skype Client Notifications for New Versions and Updates

Once the Skype application is installed, it periodically checks to see whether an update is available by default. The Skype client does not update itself. Instead, the Skype client notifies the user when a more recent copy or critical patch is available. This gives the user the option to upgrade.

Users may chose to disregard these upgrade notices. System- and network administrators may disable this feature to control software installation policies. See "Enterprise Installation and Setting Policies" below.

End users can control the Skype automatic update-notification feature by a Skype application preference (choose Tools > Options > Advanced).

Alternatively, users may manually check to see if the copy of Skype they are running is the most current version. There are two ways to accomplish this:

- A user may select Help > Check for Updates from the Skype main window. This will launch the user's default web browser and display a message indicating whether the installed version is up to date, or
- Without launching the Skype client, a user may open the Windows Control Panel and double-click on Add or Remove Programs. Then, the user can find the entry for Skype and click on the entry labeled, "Click here for support information." Follow the hyperlink on the line entitled, "Product Updates" which launches the default web browser and indicates whether the installed version is up-to-date.

Enterprise-wide Installation and Setting Policies

Skype recognizes the challenges that enterprises and other organizations face with respect to managing sophisticated IT environments, as well as the complexity related to managing all of the different software applications and hardware in use today.

Therefore, we have released a 'business version' of the Skype client, which comes with a Windows Installer Package (MSI) making it easier to deploy in an enterprise network.

You can download the business version at www.skype.com/go/businessdownload

Also, setting policies via Group Policy Objects and registry keys is now supported by Skype, please read on for more information.

Our goal is to enable system and network administrators by making it easier and by improving control over the enterprise-wide deployment and management of Skype.

Policies

The Skype client adheres to the precedence of managed settings in order of the following priority:

- 1. HKLM Registry Keys (highest precedence)
- 2. HKCU Registry Keys
- 3. shared and config.xml Skype client settings
- 4. Skype client user preferences and defaults (lowest precedence)

Windows Registry

The Skype client has end user interface controls and/or functions for many of the features over which an enterprise might want to control. Some of the more technical and network-related features and configuration options are only accessible via the registry.

This is because enterprises that require such functionality generally have systems in place for centrally managing users' registries, and registry access control to ensure that users can't circumvent such settings.

XML Configuration Files

In addition to the Windows Registry, the Skype client relies on an XML file-based setup. Administrators (and users with appropriate permissions) may open and edit these configuration files even while Skype is running.

There are two XML files - shared and private. The shared file is named shared.xml and the private file is called config.xml. Remember that XML file entries are case sensitive, so "Debug" and "debug" are different.

Note: Proper XML syntax and format (closing, opening tags, etc.) is required. Otherwise, changes will not apply or the configuration will be lost if Skype is not running.

Setting Up Group Policies

Since the release of Skype version 3.0 in 2006, it now supports the use of Group Policies to deliver and apply desired policy settings and/or configurations to a set of enterprise users and computers within a Windows Active Directory environment.

The use of Group Policies provides system and network administrators with the most convenient and reliable way to support centralized management of policy settings for Skype clients across an enterprise.

Skype policy settings set the behavior of the Skype client for a given set of targeted users or computers. Skype has been policy-enabled meaning that the behavior of the Skype client is determined and changes based on registry values indicated in an administrative template (.adm) file. This way, you can manage Skype's features and settings through registry-based policy.

Skype delivers these policy settings through a single Administrative Template file called Skype-v1.5.adm, which was designed to modify specific keys in the registry as described in the following section.

Note: You can download Skype-v1.5.adm from the Business section of the Skype website (http://www.skype.com/security/Skype-v1.5.adm) to configure Skype policies using Group Policy Editor.

Registry-based policy settings appear and may be configured in the Group Policy Object Editor, which is under the Administrative Templates node.

The Skype-v1.5.adm file does not actually apply policy settings. Instead, it simply enables you to see the policy settings in the Group Policy Object Editor. From there, you can create Group Policy objects (GPOs) that contain the policy settings which you want.

For more information on how to deliver and apply group policies, refer to:

- Open Group Policy as an MMC snap-in http://technet2.microsoft.com/WindowsServer/en/library/ae13960b-3a27-4b19-a866-ed6e6e7a312d1033.mspx?mfr=true
- Using Administrative Template Files with Registry-Based Group Policy
 http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/manageme
 nt/gp/admtgp.mspx (See "Loading an .Adm File into the Group Policy Snap-in").

Configurable Policies

Following is the list of configurable policies that apply to Skype for Windows (version 3.0 and above):

Skype Client Functionality	
DisableFileTransferPolicy	Disable file transfer to prevent the user from sending and receiving files using Skype.
DisableContactImportPolicy	Disable import contacts.
DisablePersonalisePolicy	Disable personalization to prevent the user from changing sounds.
DisableLanguageEditPolicy	Disable language edit to prevent the user from editing language strings.
WebStatusPolicy	When enabled, always publishes the user's status on the web as Skype buttons, when disabled, prevents the user from publishing status on the web.

Skype Non-functional Capabilities	
DisableApiPolicy	Disable Skype Public API to prevent third- party applications from accessing Skype functionality.
DisableVersionCheckPolicy	Disable new version checking by preventing Skype from detecting new versions and updates.
MemoryOnlyPolicy	Run in memory-only mode so Skype does not store any data on the local disk.
Network-related Functionality	
ListenPortPolicy	Set the listening port where Skype listens for incoming connections.
ListenPort	Listening port number.
ListenHTTPPortsPolicy	When enabled, listen on HTTP (port 80) and HTTPS (port 443) ports; when disabled, don't listen on HTTP/HTTPS ports; when not configured, let the user decide.
DisableTCPListenPolicy	Disable listening for TCP connections to prevent the Skype client from receiving incoming TCP connections.
DisableUDPPolicy	Disable UDP communications to prevent the Skype client from using UDP to communicate with the network.
DisableSupernodePolicy	Prevent the Skype client from becoming a supernode.
ProxyPolicy	Establish the proxy policy.
ProxyType	Establish the proxy type.
ProxyUnset	Unset
ProxyAutomatic	Automatic
ProxyDisabled	Disabled
ProxyUnset	Unset
ProxyHTTPS	HTTPS
ProxySOCKS5	SOCKS5
ProxyAddress	Proxy address (host:port)
ProxyUsername	Username
ProxyPassword	Password

Registry Keys

Following is the list of registry keys that apply to the Skype for Windows (version 3.0 and above):

HKEY_LOCAL_MACHINE (HKLM)

The registry keys for the local machine take precedence over the registry keys for the local user if there is a conflict.

```
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableApi, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableFileTransfer, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, MemoryOnly, REG DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableContactImport, REG_DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableVersionCheck, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisablePersonalise, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableLanguageEdit, REG DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ListenPort, REG_DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, ListenHTTPPorts, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableTCPListen, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableUDP, REG DWORD = {0,1}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, DisableSupernode, REG DWORD = {0,1}
HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, ProxyAddress, REG SZ = {string}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, ProxyUsername, REG SZ = {string}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, ProxyPassword, REG SZ = {string}
HKEY LOCAL MACHINE\Software\Policies\Skype\Phone, WebStatus, REG DWORD = {0,1}
```

HKEY_CURRENT_USER (HKCU)

The registry keys for the current user take precedence over the configuration parameters in the XML configuration files if there is a conflict.

The configuration parameters defined in the XML configuration files shared.xml and config.xml take precedence over any preferences the user selects in the Skype client if there is a conflict.

```
HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableApi, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableFileTransfer, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, MemoryOnly, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableContactImport, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableVersionCheck, REG_DWORD = {0,1}
```

```
HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisablePersonalise, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableLanguageEdit, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ListenPort, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ListenHTTPPorts, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableTCPListen, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableUDP, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableSupernode, REG_DWORD = {0,1}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, WebStatus, REG_DWORD = {0,1}
```